REMARKS

The present application was filed on September 15, 2005, with claims 1-40. The present application claims priority to PCT application US04/21846, filed July 9, 2004, and U.S. provisional application Serial No. 60/486,127, filed July 10, 2003. Claims 1-40 remain pending in the present application.

Claims 1, 2, 5, 6, 13, 19 and 35-40 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,298,851 (hereinafter "Hendricks").

Claims 3, 4, 7-12, 14-18 and 20-34 are each rejected under 35 U.S.C. §103(a) over Hendricks in view of one or more other cited references.

In this response, Applicants traverse the §103(a) rejections.

With regard to the §103(a) rejection over Hendricks, the Examiner argues that each and every limitation in claims 1, 2, 5, 6, 13, 19 and 35-40 is taught or suggested by Hendricks. Applicants respectfully disagree.

Independent claim 1 is directed to a method for secure generation of a seed for use in performing one or more cryptographic operations. The method includes the steps of a seed generation server providing a first string to a seed generation client, the seed generation client generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server, the seed generation client generating the seed as a function of at least the first string and the second string, and the seed generation server decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string.

An important advantage of the claimed arrangement is that it overcomes the problems associated with conventional seed generation techniques that may result in the seed becoming accessible in plaintext form to entities other than an authentication token and an authentication entity. See the specification at, for example, page 2, lines 1-14, page 3, lines 10-13, and page 6, lines 5-7.

The Examiner in formulating the §103(a) rejection of claim 1 argues that the limitations of claim 1 are met by the teachings in column 42, lines 1-15, of Hendricks, relating to a key agreement protocol. See the final Office Action dated November 10, 2009 at page 4, lines 1-10. Applicants respectfully disagree. This portion of Hendricks provides as follows:

> In a different embodiment, depicted in FIG. 24b, the publisher 282 serves as the sender 4998 and operations center 250 serves as the recipient 4999. Initial key negotiation information 5200 is exchanged between a seed key generation algorithm 5201 at the publisher 282 and a seed key generation algorithm 5202 at the operations center 250. As a result, the seed key generation algorithm 5201 at the publisher 282 and the seed key generation algorithm 5202 at the operations center 250 each generate seed key SK 5203 using, for example, the Elliptic Curve Diffie-Hellman key exchange algorithm, as described in U.S. Pat. No. 4,200,700. The seed key SK 5203 is then used by key sequence generator 5204 at the publisher 282 to generate the first in a sequence of keys, transaction symmetric key SKTi 5206.

The relied-upon portion of Hendricks simply indicates that the sender 4998 and recipient 4999 in FIG. 24b generate a shared key 5203 using the conventional Diffie-Hellman key exchange algorithm. However, the Diffie-Hellman key exchange algorithm does not operate in the manner recited in claim 1. In other words, the Diffie-Hellman key exchange algorithm does not involve a first entity providing a first string to a second entity, the second entity generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the first entity, the second entity generating the seed as a function of at least the first string and the second string, and the first entity decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string. To the contrary, the Diffie-Hellman key exchange algorithm is summarized in column 2, lines 35-52, of U.S. Patent No. 4,200,770 as follows:

> In the present invention a first converser transforms, in a manner infeasible to invert, a first signal while a second converser transforms, also in a manner infeasible to invert, a second signal. The first converser transmits the transformed first signal to the second converser, keeping the first signal secret, and the second converser transmits the transformed second signal to the first converser, keeping the second signal secret. The first converser then transforms the first signal with the transformed second signal to generate a third signal, representing a secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. And, the second converser transforms the second signal with the transformed first signal to generate a fourth signal, also representing the secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal.

In the November 10, 2009 Office Action, at pages 2-3, section 4, the Examiner addresses the foregoing arguments by referring to teachings from another reference, V. Boyko et al., "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," (hereinafter "Boyko"). Applicants initially note that the rejection in question is a §103(a) rejection over Hendricks alone, and not a §103(a) rejection over a combination of Hendricks and Boyko. This is believed to be entirely inappropriate. MPEP 706.02(j) provides as follows, with emphasis supplied:

> Where a reference is relied on to support a rejection, whether or not in a minor capacity, that reference should be positively included in the statement of the rejection. See *In re Hoch,* 428 F.2d 1341, 1342 n.3 166 USPQ 406, 407 n. 3 (CCPA 1970).

Accordingly, if the Examiner requires teachings from Boyko in order to meet all of the limitations of claim 1, for example, the proper course of action is to withdraw the §103(a) rejection over Hendricks alone, and issue a new §103(a) rejection over the combination of Hendricks and Boyko.

Moreover, any such new rejection should be made non-final, as Applicants did not amend the claims in their previous response filed June 22, 2009, nor did Applicants submit the Boyko reference in an information disclosure statement. See MPEP 706.07(a), which provides as follows, again with emphasis supplied:

> Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims, nor based on information submitted in an information disclosure statement filed during the period set forth in 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p). Where information is submitted in an information disclosure statement during the period set forth in 37 CFR 1.97(c) with a fee, the examiner may use the information submitted, e.g., a printed publication or evidence of public use, and make the next Office action final whether or not the claims have been amended, provided that no other new ground of rejection which was not necessitated by amendment to the claims is introduced by the examiner. See MPEP § 609.04(b). Furthermore, a second or any subsequent action on the merits in any application or patent undergoing reexamination proceedings will not be made final if it includes a rejection, on newly cited art, other than information submitted in an information disclosure statement filed under 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p), of any claim not amended by applicant or patent owner in spite of the fact that other claims may have been amended to require newly cited art. Where information is submitted in a reply to a requirement under 37 CFR 1.105, the examiner may NOT make the next Office action relying on that art final unless all instances of the application of such art are necessitated by amendment.

It is therefore believed that if the Examiner wishes to rely on the Boyko reference to support the §103(a) rejection over Hendricks, that rejection must be withdrawn and a new non-final rejection over Hendricks and Boyko should be issued.

Although Applicants believe it was improper for the Examiner to rely on Boyko in the manner set forth in the present Office Action, that reference fails to supplement the teachings of Hendricks in a manner that would meet the limitations of claim 1. As Applicants noted above, FIG. 24b of Hendricks shows an arrangement in which sender 4998 and recipient 4999 generate a shared key 5203 using the conventional Diffie-Hellman key exchange algorithm. The initial key negotiation information is information exchanged in accordance with the Diffie-Hellman key exchange algorithm. The Examiner with reference to Boyko relies primarily on the EKE teachings at pages 158-159. See the Office Action at page 3, lines 2-12. However, this portion of Boyko provides as follows, with emphasis supplied and citations omitted:

> The EKE protocol was the first password authenticated key exchange protocol that did not require the user to know the server's public key. The idea of EKE was to use the password to symmetrically encrypt the protocol messages of a standard key exchange (e.g., Diffie-Hellman). Then an attacker making a password guess could decrypt the symmetric encryption, but could not break the asymmetric encryption in the messages, and thus could not verify the guess.

Thus, the EKE protocol does not modify the underlying Diffie-Hellman protocol in any way, but instead just calls for encrypting the messages of the Diffie-Hellman protocol using a password known to both parties. As Applicants noted above, the Diffie-Hellman protocol does not operate in the manner recited in claim 1, and this remains true even if one were to encrypt all of the Diffie-Hellman protocol messages in accordance with the EKE teachings from Boyko. More specifically, in the claimed arrangement, a first entity provides a first string to a second entity, the second entity generates a second string, encrypts the second string utilizing a key, and sends the encrypted second string to the first entity, with the second entity generating the seed as a function of at least the first string and the second string, and the first entity decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string. If one were to encrypt the Diffie-Hellman protocol messages in accordance with the EKE teachings from Boyko, the following would apparently be the result, based on the previously-quoted description summarized in column 2, lines 35-52, of U.S. Patent No. 4,200,770, with the modifications associated with EKE encryption and decryption shown in italics:

> In the present invention a first converser transforms, in a manner infeasible to invert, a first signal while a second converser transforms, also in a manner infeasible to invert, a second signal. The first converser *encrypts the transformed first signal and* transmits the *encrypted* transformed first signal to the second converser, keeping the first signal secret, and the second converser *encrypts the transformed second signal and* transmits the *encrypted* transformed second signal to the first converser, keeping the second signal secret. The first converser then *decrypts the transformed second signal and* transforms the first signal with the *decrypted* transformed second signal to generate a third signal, representing a secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. And, the second converser *decrypts the transformed first signal and* transforms the second signal with the *decrypted* transformed first signal to generate a fourth signal, also representing the secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal.

Assume for purposes of argument that the recited first and second strings of claim 1 are alleged to be met by the transformed first signal and the transformed second signal, respectively, of the modified Diffie-Hellman protocol above, and further that the recited seed generation server and seed generation client are alleged to be met by the first converser and second converser, respectively. However, claim 1 recites that the seed generation server generates the seed as a function of at least the first string and the second string. In the Diffie-Hellman protocol, the first converser generates a secure cipher key by transforming the first signal using the transformed second signal. Thus, the first converser does not generate the secure cipher key as a function of the transformed first signal (alleged to meet the first string) and the transformed second signal (alleged to meet the second string). Similarly, claim 1 recites that the seed generation client generates the seed as a function of at least the first string and the second string. In the Diffie-Hellman protocol, the second converser generates a secure cipher key by transforming the second signal using the transformed first signal. Thus, the second converser does not generate the secure cipher key as a function of the transformed first signal (alleged to meet the first string) and the transformed second signal (alleged to meet the second string). It is therefore apparent that the collective teachings of Hendricks and Boyko fail to meet the limitations of claim 1.

Accordingly, it is apparent that simply encrypting the messages of the conventional Diffie-Hellman protocol based on the EKE teachings of Boyko would not result in an arrangement that meets the particular limitations of claim 1.

Therefore, even if the Examiner were to issue an appropriate rejection over Hendricks and Boyko, the collective teachings of those references would fail to meet the limitations in question.

The §103(a) rejection of claim 1 over Hendricks is therefore believed to be improper and should be withdrawn.

Independent claims 35-40 include limitations similar to those of claim 1, and are believed allowable for reasons similar to those outlined above in the context of claim 1.

Dependent claims 2-34 are believed allowable at least by virtue of their dependence from claim 1, and are also believed to define separately-patentable subject matter. The additional references cited by the Examiner fail to supplement the fundamental deficiencies of the Hendricks reference as applied to claim 1.

In view of the foregoing, claims 1-40 are believed to be in condition for allowance.

Respectfully submitted,

Joseph B. Ryan

Date: January 11, 2010

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517